

REMARKS

The Examiner has rejected Claims 1-4, 15-16, and 20-24 under 35 U.S.C. 102(e) as being anticipated by Redlich (USPN 6,591,306). Applicant respectfully disagrees with such rejection, especially in view of the incorporation of the subject matter of Claims 5-6 et al. (or substantially similar, but not identical, language) into each of the independent claims.

The Examiner has rejected the subject matter of former Claims 5-6 (now substantially incorporated into each of the independent claims), as well as Claims 7-14, 17-19, and 25-29 under 35 U.S.C. 103(a) as being unpatentable over Redlich (USPN 6,591,306) in view of Underwood (USPN 6,704,873). Applicant respectfully disagrees with this rejection.

For example, the Examiner relies on the following excerpt from Underwood to make a prior art showing of applicant's claimed "wherein forwarding said request comprises: determining whether an attack is consuming significant resources, if it is determined that an attack is not consuming significant resources, slowing down the forwarding of said request short of stopping the same, and if it is determined that an attack is consuming significant resources, stopping the forwarding of said request" (see this or similar, but not identical claim language in each of the independent claims).

"The screening router denies typical attacks caused by malicious manipulation of EP options flags in the IP header, such as source routing and fragmentation attacks." (see col. 284, lines 48-50)

Moreover, the Examiner notes that "the denial of data packets will automatically slow down the system." Applicant respectfully disagrees with this assertion. Slowing down the system is much different than blocking packets. To further emphasize the distinction between applicant's claimed slowing, applicant now claims slowing "short of stopping."

Only applicant teaches and claims a two-prong response (including stopping and slowing) based, specifically, on a determination as to whether an attack is consuming significant resources, as claimed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness has not been met. For example, with respect to the third element of the *prima facie* case of obvious, such element has not been met since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the Examiner's application of the prior art to applicant's remaining dependent claims is further replete with deficiencies. Just by way of example, the Examiner relies on the following excerpt from Underwood to make a prior art showing of applicant's claimed "tracking down a source of the attack," "wherein tracking down a source of the attack comprises performing a trace back at the secret host" (see Claims 8-9).

"In the Data Communications review, they rated the ease of performing certain tasks using each product. These tasks include configuring alert notification, remote shutdown, denying access from a given subnet, log blocked access attempts, and various common rules." (col. 266, lines 44-47)

Applicant respectfully disagrees with this assertion. There is simply not even a suggestion of tracing by Underwood in a security context, let alone tracking down a source of the attack, wherein tracking down a source of the attack comprises performing a trace back at the secret host.

Further, the Examiner relies on col. 226, lines 49-50; and col. 228, lines 35-37 and 45-46 from Underwood to make a prior art showing of applicant's claimed "wherein a notification that the public host is under attack is received at the secret host," and "wherein a notification that the public host is congested is received at the secret host" (see Claims 11-12). Applicant respectfully disagrees with this assertion. Underwood does not even make a mention of a secret host, let alone a secret host that receives either of the specific notifications, as claimed.

Still yet, the Examiner relies on the following excerpt from Redlich to make a prior art showing of applicant's claimed "code that directs one or more clients to send requests to an alternate public host upon receiving said notification," and "code that requests the DNS server to replace the public host address with an alternate public host address upon receiving said notification" (see Claims 18-19).

"On a LINUX system, for instance, the guest could create additional secure tunnels to other trusted routers in the Internet. Those additional tunnels could be used as alternative routes for outbound traffic." (col. 24, lines 53-57)

Applicant respectfully disagrees with this assertion. There is simply not even a suggestion of the specifically claimed "requests" that are put in place upon receiving the particularly claimed notification.

Even still, the Examiner relies on the following excerpt from Redlich to make a prior art showing of applicant's claimed "wherein the secret host is configured to manage the public host" (see Claim 21).

"Each of the stations 310-340 shown in FIG. 3 may be a digital computer 10 as shown in FIG. 1. The stations 310-340 can all communicate with each other by virtue of the second network 300, but cannot communicate with any of the stations 210-240 of the first network 200, in the arrangement shown in FIG. 3. This is because there is no interconnection between network 200 and network 300." (col. 3, lines 62-67)

Applicant again respectfully disagrees with this assertion. There is simply not even a suggestion of any sort of configuration of a secret host so as to manage a public host, as claimed.

The Examiner also relies on col. 228, lines 45-46 from Underwood to make a prior art showing of applicant's claimed "switching to an alternate public host when congestion at the public host exceeds a predetermined level" (see Claims 28). Applicant respectfully disagrees with this assertion. There is simply not even a suggestion of any sort of switching to an alternate public host, when congestion at the public host exceeds a predetermined level, in the context of the claimed invention.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the following additional dependent claims that have been added for full consideration:

"wherein, after stopping the forwarding of said packets, said secret node requests that the DNS server replace a current public node IP address with an IP address of an alternate public node, and attempts to track down a source of the attack, where, after the attack has stopped, an IP address of an alternate Post Office Box Internet Protocol (POBIP) node is replaced with an original public node IP address" (see Claim 30); and

"wherein, after stopping the forwarding of said packets, said secret node notifies select clients of an alternate public node IP address, and attempts to track down a source of the attack, where, after the attack has stopped, an IP address of an alternate Post Office Box Internet Protocol (POBIP) node is replaced with the IP address of the public node" (see Claim 31).

Again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P310).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100